JOURNAL OF COMBINATORIAL THEORY, Series A 52, 188–196 (1989)

Affine Difference Sets of Even Order

K. T. ARASU*

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

AND

DIETER JUNGNICKEL†

Mathematisches Institut, Justus-Liebig-Universität Giessen, Arndtstrasse 2, 6300 Giessen, Federal Republic of Germany

Communicated by Marshall Hall, Jr.

Received December 15, 1987

Generalizing a result of Ko and Ray-Chaudhuri (*Discrete Math.* **39** (1982), 37–58), we show the following: Assume the existence of an affine difference set in G relative to N of even order $n \neq 2$. If G is of the form $G = N \oplus H$, where N is abelian, then n is actually a multiple of 4, say $n = 4k$, and there exists a $(4k-1, 2k-1, k-1)$-Hadamard difference set in N. More detailed considerations lead to variations of this result (under appropriate assumptions) which yield even stronger non-existence theorems. In particular, we show the non-existence of abelian affine difference sets of order $n \equiv 4 \bmod 8$ (with the exception $n = 4$) and of nilpotent affine difference sets of order $n \equiv 2 \bmod 4$ ($n \neq 2$). The latter result is the first general non-existence theorem in the non-abelian case.

1. INTRODUCTION

Let D be an affine difference set of order n in a group G (of order $n^2 - 1$) relative to a (normal) subgroup N (of order $n - 1$) of G. Thus D is an n-subset of G for which the list of differences $d - d'$ $(d, d' \in D, d \neq d')$ contains each element of $G - N$ exactly once, and therefore contains no element of N. We shall call D *splitting* if G is of the form $G = N \oplus H$. (We write G additively, even if G is non-abelian.) One can use the Desarguesian affine plane of order q (q a prime power) to construct a cyclic affine difference set of order q; see Bose [3]. The prime power conjecture states that these are the only orders for which (cyclic) affine difference sets exist, cf.

* Research supported in part by National Security Agency Grant MDA904-87-H-2018.

† The second author thanks both Wright State University and the University of Waterloo for their hospitality during the time of this research. He also gratefully acknowledges the financial support of NSERC under Grant IS-0367.

0097-3165/89 $3.00

Hoffman [7]. Despite considerable effort and several non-existence results (see, e.g., [1, 7, 9, 12, 13, 16]) this conjecture remains unsolved though it is verified for order $\leqslant 5000$ (see [12]). The first major progress for even orders n was obtained by Ko and Ray-Chudhuri [13] who proved the following result.

THEOREM 1. *Let D be a cyclic affine difference set of even order $n \neq 2$. Then n is divisible by 4, say $n = 4k$, and there exists a cyclic Hadamard difference set of order k, i.e., a cyclic $(4k-1, 2k-1, k-1)$-difference set.*

The first part of Theorem 1 has been generalized by Jungnickel [9] to abelian affine difference sets; see also [1, 16] for proofs of this result. In the present paper, we shall generalize both parts of Theorem 1 to the abelian case and, in fact, also to certain non-abelian splitting affine difference sets (see Theorem 2). This already suffices to obtain an elementary proof for the non-existence of affine difference sets in infinitely many non-abelian groups. We then use a generalization of Theorem 2 which can be applied to prove the non-existence of any splitting (hence, in particular, of any nilpotent) affine difference set of order $n \equiv 2 \bmod 4$. This seems to require the use of the Feit–Thompson theorem. We thus obtain the first general non-existence theorem for non-abelian affine difference set, which is of considerable interest as it is a common experience that it is much more difficult to obtain non-existence results for difference sets and relative difference sets in the non-abelian case than in the abelian case; the main reason for this fact is the lack of any efficient theory of multipliers in the general case.

In the final section we analyse the proof of Theorem 2 in more detail in the special case of abelian groups. Considering multipliers, we can considerably strengthen our result; in particular, n will necessarily be a multiple of 8 (unless $n = 4$). We also obtain further restrictions.

2. THE MAIN RESULT

In this section, we shall prove the following Theorem 2; some first applications will be given in Section 3.

THEOREM 2. *Let $G = H \oplus N$ be an additively written group, where H is any group of order $n+1$ and where N is an abelian group of order $n-1$, and assume the existence of an affine difference set S in G (relative to N). If n is even $(n \neq 2)$, then n is divisible by 4, say $n = 4k$, and there exists a $(4k-1, 2k-1, k-1)$-difference set in N.*

Proof. Let $S = \{(h_i, n_i): h = 1, ..., n\}$ and note that the h_i are pairwise distinct (by definition of an affine difference set).

We use S to construct a certain $(n+1)\times(n+1)$-matrix $A=(a_{gh})$ with entries from $N\cup\{\infty\}$, where the rows and columns are labelled with the elements of H: If $(g, m)\in S$, put

$$a_{g+h,h}=m \qquad \text{for all } h\in H;$$

the remaining entries of A are ∞. Since we may assume $S\cap N=\varnothing$, we can ensure that the unique entry ∞ in row 0 of A is a_{00}; so in general the entries ∞ occur in the positions (h, h), $h\in H$. (This is not essential but will somewhat simplify the following computations.) By construction, A is an H-invariant matrix; i.e., we have

(1) $a_{f+h,\,g+h}=a_{fg}$ for all $f, g, h\in H$.

We now claim the following:

(2) $\{a_{fj}-a_{gj}: j\in H, j\neq f, g\}=N$ for all pairs f, g of distinct elements of H.

For proof, note first that $a_{fj}-a_{gj}=a_{0,j-f}-a_{g-f,j-f}$ by (1); thus it suffices to prove (2) in the special case $f=0$. Now let $x\in N$ be arbitrary; for reasons of cardinality, it suffices to show that x has some representation of the form $x=a_{0j}-a_{gj}$ $(j\neq 0, g)$. By definition of an affine difference set, there exist $d=(h, m)$ and $d'=(h', m')$ in S such that

$$d-d'=(h-h', m-m')=(-g, x),$$

i.e., $h'=g+h$ and $m'=-x+m$. By our construction of A, we thus have $a_{h,0}=m$ and $a_{g+h,0}=-x+m$; then (1) yields $a_{0,-h}=m$ and $a_{g,-h}=-x+m$, hence $a_{0,-h}-a_{g,-h}=x$, as required.

We next claim that

(3) $a_{0,-h}=a_{0h}$ for all $h\in H$.

For proof, consider the set of differences

$$\{a_{0j}-a_{hj}: j\neq 0, h\}=N=\{a_{0j}-a_{0,j-h}: j\neq 0, h\}$$

(by (1) and (2)). Adding all these differences yields (since (N) is odd) the equation

$$0=\sum_{m\in N} m=a_{0,-h}-a_{0,h},$$

as desired. We now put $d_j:=a_{0j}$ for all $j\in H\setminus\{0\}$ and claim:

(4) the list of all differences d_i-d_j $(i, j\in H\setminus\{0\}, i\neq j)$ contains each element of N exactly n times.

For proof, note that by definition we have to consider the list of differences $a_{0i}-a_{0j}$ $(i\neq j, i, j\neq 0)$ which by (1) is the list of all differences

$a_{-i+j,j} - a_{0,j}$. Now $c \in H \setminus \{0\}$; then for each $j \neq c$ there is a unique $i \neq 0, j$ such that $c = -i + j$. Hence our list of differences can be written as the union (over all $c \in H \setminus \{0\}$) of the lists

$$a_{cj} - a_{0j} \qquad (j \in H, j \neq 0, c);$$

but each such list contains each element of N exactly once, by (2), which proves (4).

We now switch to multiplicative notation for N, since we want to use the group algebra $\mathbb{Q}N$. Thus we rewrite (4) as

(4′) The list of all $d_i d_j^{-1} (i, j \in H \setminus \{1\}, i \neq j)$ contains each element of N exactly n times.

Define $D \in \mathbb{Q}N$ by $D = \sum_{i \in H \setminus \{0\}} d_i$. Then (4′) implies

(5) $DD^{(-1)} = n + nN,$

where (as usual) we write $D^{(-1)} = \sum_{d \in D} d^{-1}$ and denote by N also the sum $\sum_{m \in N} m$ of all the elements of N in $\mathbb{Q}N$. Now let $\tilde{H}$ denote a system of representatives for the set

$$\{\{x, -x\} : x \in H, x \neq 0\},$$

and put $B = \sum_{x \in \tilde{H}} d_x$. Then (3) implies $D = 2B$ in $\mathbb{Q}N$ and thus (5) may be rewritten as

(6) $4BB^{(-1)} = n(1 + N).$

This shows that n is divisible by 4, say $n = 4k$. Then (6) finally yields

(7) $BB^{(-1)} = k + kN;$

since the coefficient of 1 in (7) is $2k$, we see that the elements $\{d_x : x \in \tilde{H}\}$ are pairwise distinct. But then (7) means that the set $B = \{d_x : x \in \tilde{H}\}$ is a $(4k - 1, 2k, k)$-difference set in N (see, e.g., Beth, Jungnickel, and Lenz [2] for background on difference sets and group algebras). So the complementary difference set $\bar{B} = N - B$ is the desired Hadamard difference set in N.

Remarks. The matrix A defined above is, in the terminology of Jungnickel [8], a generalized balanced weighing matrix GBW$(n - 1, n + 1, n)$ over N, since it satisfies Eq. (2). In fact, (2) follows from a much more general result of [8], where it has been shown that any relative difference set with parameters (n, m, k, λ) in a group of the form $G = H \oplus N$ is equivalent to an H-invariant GBW(n, m, k) over N. To make this paper self-contained, we have preferred to avoid quoting the results of [8]. It should also be noticed that our proof of Theorem 2 is somewhat similar to the proof of Theorem 1 given by Ko and Ray-Chaudhuri [13] who also construct a GBW-matrix. However, our proof is simpler as it avoids constructing the desired matrix by a series of transformations.

3. Some Applications

In this section we give a few applications of Theorem 2 which will already imply the non-existence of affine difference sets for infinitely many cases not covered by the results of [13]. In the following two sections, we shall considerably strengthen our results; in particular, Corollaries 1 and 2 below are only preliminary steps. We first note the following generalization of Theorem 1, which we announced in the introduction:

Corollary 1. *Let D be an abelian affine difference set of order n in G, relative to N. If $n \neq 2$ is even, then n is divisible by 4, say $n = 4k$, and there exists a Hadamard difference set of order k in N.*

For proof, note that $|N| = n - 1$ and $n + 1$ are coprime, as a is even. Thus G splits as $G = H \oplus N$, where H is the unique subgroup of order $n + 1$ of G, and Theorem 2 applies.

Example 1. Let $n = 76$ and let N be any abelian group of order 75. It is well known that N does not contain a Hadamard difference set (see the tables in [2] or [14]). Thus no abelian affine difference set of order 76 exists; note that there is a non-cyclic example ($N = \mathbf{Z}_5 \oplus \mathbf{Z}_5 \oplus \mathbf{Z}_3$) which thus is not already ruled out by Theorem 1.

Example 2. Similarly, let $n = 56$. Again, there is no Hadamard difference set in $N = \mathbf{Z}_{55}$ (see [2] or [14]). By Theorem 2, no affine difference set of order 56 in any group of the type $G = H \oplus \mathbf{Z}_{55}$ (H a group of order 57) can exist. Since $57 = 3 \cdot 19$ and since 3 divides 18, there is a non-abelian group H of order 57. We thus get the non-existence of an affine difference set in $H \oplus \mathbf{Z}_{55}$, a result not previously known.

Corollary 2. *Let N be any abelian group of order $n - 1$, where $n \equiv 2 \bmod 4$, and let H be any group of order $n + 1$. Then $G = H \oplus N$ does not admit an affine difference set of order n.*

Example 3. Let p be a prime $\equiv 3 \bmod 4$. By Dirichlet's theorem, there exist infinitely many primes q of the form $q = 4ap + 1$. Then $p \mid q - 1$, and thus there exists a non-abelian group $H = \mathbf{Z}_p \cdot \mathbf{Z}_q$ of order $n + 1 = n(p, q) + 1 = p(4ap + 1) \equiv 3 \bmod 4$. Thus $n = n(p, q) \equiv 2 \bmod 4$ and we obtain the non-existence of affine difference sets in $H \oplus N$, where N is any abelian group of order $n - 1$, by Corollary 2. Thus out result rules out infinitely many non-abelian cases previously open. Of course, one can also use primes $p \equiv 1 \bmod 4$ and primes $q = 4ap + (2p + 1) \equiv 3 \bmod 4$. Some small numerical examples include $n = 38, 50, 86, \ldots$ (for $p = 3$) and $n = 54, 154, \ldots$ (for $p = 5$).

4. A Generalization

Let D be an affine difference set of order n, i.e., a relative difference set (RDS) with parameters $(n-1, n+1, n, 1)$, in a group G (relative to N); cf. [4, or 8] for relative difference sets. Assume the existence of a normal subgroup $M \subseteq N$ of G of order λ. Then projection of D into G/M yields a relative difference set $\bar{D}$ with parameters $((n-1)/\lambda, n+1, n, \lambda)$ in G/M (relative to N/M). But whereas the existence of D in G yields the existence of a projected relative difference set in G/M, we cannot conclude anything about the non-existence of an $((n-1)/\lambda, n+1, n, \lambda)$-RDS in G/M from the non-existence of an affine difference set in G. It is, however, possible to generalize the first part of Theorem 2 to obtain the following non-existence result for $((n-1)/\lambda, n+1, n, \lambda)$-RDSs.

Theorem 3. *Let $G = H \oplus N$, where H is any group of order $n+1$ and where N is an abelian group of order $(n-1)/\lambda \neq 1$, and assume the existence of an $((n-1)/\lambda, n+1, n, \lambda)$-RDS in G (relative to N). If n is even, then n is divisible by 4.*

Proof. The proof of Theorem 2 carries over to this more general situation, with a few minor modifications. For instance, (2) now should read

(2′) The list of differences $a_{fj} - a_{gj}$ $(j \in H,\ j \neq f, g)$ contains each element of N exactly λ times (for all pairs f, g of distinct elements of H).

And (6) becomes

(6′) $4BB^{(-1)} = n(1 + \lambda N)$.

Therefore we again infer that n is divisible by 4.

The main interest of Theorem 3 lies in the fact that it can be used to considerably strengthen Corollary 2 by using the projection construction mentioned at the beginning of this section on a hypothetical affine difference set D of order $n \equiv 2 \bmod 4$ in $G = H \oplus N$. To this end it suffices to assume that N admits a non-trivial abelian homomorphic image, i.e., that the commutator subgroup N' of N is a proper subgroup of N. Then $K = H \oplus M$ (with $M = N/N'$) satisfies the hypothesis of Theorem 3 (with $\lambda = |N'|$) and we obtain the contradiction $n \equiv 0 \bmod 4$. Note that $N' \neq N$ whenever N is a solvable group. Since $|N|$ is odd, however, this assumption is always satisfied, by the theorem of Feit and Thompson [5]. Thus we have the following improvement of Corollary 2:

Theorem 4. *Let $n \equiv 2 \bmod 4$. Then there is no splitting difference set of order n.*

While this result is non-elementary (since it uses the deep Feit–Thompson theorem), the following corollary is elementary (noting that any nilpotent group of order n^2-1, n even, splits as $G=N\oplus H$ (with $|N|=n-1$) and is solvable):

COROLLARY 3. *There exists no nilpotent affine difference set of order* $n\equiv 2 \bmod 4$.

Note that there do exist non-abelian affine difference sets; Ganley and Spence [6] have constructed examples of order n for any odd prime power n.

5. THE ABELIAN CASE

In this final section we shall considerably strenghthen Corollary 1 by proving the following result:

THEOREM 5. *Assume the existence of an abelian affine difference set in G (relative to N). If n is even and* $n\neq 2, 4$, *then n is in fact a multiple of* 8. *Moreover, the following two conditions have to be satisfied:*

(i) *There exists a Hadamard difference set in N which admits every prime divisor of n as a multiplier.*

(ii) *Either n is a square, or we have* $(p/q)=1$ *for each prime p dividing n and each prime q dividing* $n-1$. *(Here* (p/q) *denotes the Legendre symbol.)*

Proof. Since n is even, we may write G as $G=H\oplus N$. The proof consists of elaborating the proof of Theorem 2. Since G is abelian, each prime p dividing n is a multiplier of the affine difference set S in G. We may assume that S is fixed by all such primes p (if necessary, we can replace D by a suitable translate). This assumption however makes it impossible to also assume that $a_{00}=\infty$. We will now show that actually this condition has to be satisfied if D is fixed under the multiplier 2. Let c be the unique index in H with $a_{0c}=\infty$; thus the entry ∞ in row g of A occurs as $a_{g,c+g}$ by (1). We then have to modify (2) as follows:

(2′) $\{a_{fj}-a_{gj}: j\in H,\ j\neq c+f, c+g\}=N$ for all pairs f, g of distinct elements of H;

the proof of (2) carries over. Instead of (3), the same reasoning will now yield

(3′) $a_{0,c+h}=a_{0,c-h}$ for all $h\in H$.

Moreover, since S is fixed under the multiplier 2, we have $(2g, 2m) \in S$ whenever $(g, m) \in S$; this implies

$$2a_{g,0} = a_{2g,0} \qquad \text{for all } g \in H \tag{*}$$

(by construction of A). Using (*), (1), and (3′) with $h = c$, we obtain

$$a_{00} = a_{0,c-c} = a_{0,c+c} = a_{0,2c} = a_{-2c,0} = 2a_{-c,0} = 2a_{0c} = 2\infty = \infty,$$

as claimed. Thus (3) is in fact still valid.

We now construct D and B as before, and consider an arbitrary prime p dividing n. Then (*) generalizes to

$$pa_{g,0} = a_{pg,0} \qquad \text{for all } g \in H$$

which implies (using (1))

$$pd_j = d_{pj} \qquad \text{for all } j \in H. \tag{**}$$

Thus the multiplier group of S carries over to D. In group algebra notation (switching to multiplicative notation for G, once more) (**) reads

$$D^{(p)} = D \qquad \text{in } \mathbb{Q}G;$$

but, as we noted in the proof of Theorem 2, $D = 2B$, and therefore clearly also

$$B^{(p)} = B,$$

since $(2B)^{(p)} = 2B^{(p)}$. Thus p is a multiplier of B, and therefore also of the complementary (Hadamard) difference set $\bar{B}$ in N. This proves (i).

We first consider the case $p = 2$. Thus there is a $(4k-1, 2k-1, k-1)$ difference set with multiplier 2 in N. But this implies that $k = (2k-1) - (k-1)$ is divisible by 2, by a result due to Ko [11] and Pott [17] (which ensures that 2 is never an extraneous multiplier for a non-trivial abelian difference set). Hence n is a multiple of 8, as claimed.

Finally, let p be an arbitrary prime dividing n, again. We have proved the existence of a Hadamard difference set with multiplier p in N. Since $4k-1$ and k are coprime, a well-known result of Mann [15] (see also [2]) implies that either n is a square or p has odd order mod (exp N); the latter condition is equivalent to saying that $(p/q) = 1$ for each prime divisor of $n-1$. This finishes the proof of Theorem 5.

Remark. The divisibility assertion of Theorem 5 is the affine analogue of the theorem of Jungnickel and Vedder [10]: An abelian planar difference set of even order $n \neq 2, 4$ can only exist if n is a multiple of 8. Note

that the known proofs of these similar results are radically different. For example, a crucial step in [10] is the following lemma: The existence of an abelian planar difference set of order n^2 implies that of such a set of order n. No affine analogue of this lemma is known. It is rather curious that the only other known general non-existence result also applies to both planar and affine abelian difference sets of order n: If n is a multiple of 3, then $n = 3$ or n is divisible by 9 (see Wilbrink [18] and Pott [16], respectively).

REFERENCES

1. K. T. ARASU, Cyclic affine planes of even order, *Discrete Math.*, in press.
2. T. BETH, D. JUNGNICKEL, AND H. LENZ, "Design Theory," Bibliograph. Inst., Mannheim, 1985; Cambridge Univ. Press, Cambride, 1986.
3. R. C. BOSE, An affine analogue of Singer's theorem, *J. Indian Math. Soc.* **6** (1942), 1–15.
4. J. E. H. ELLIOTT AND A. T. BUTSON, Relative difference sets, *Illinois J. Math.* **10** (1966), 517–531.
5. W. FEIT AND J. G. THOMPSON, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 755–1029.
6. M. J. GANLEY AND A. SPENCE, Relative difference sets and quasi-regular collineation groups, *J. Combin. Theory Ser. A* **19** (1975), 134–153.
7. A. J. HOFFMAN, Cyclic affine planes, *Canad. J. Math.* **4** (1952), 295–301.
8. D. JUNGNICKEL, On automorphism groups of divisible designs, *Canad. J. Math.* **34** (1982), 257–297.
9. D. JUNGNICKEL, A note on affine difference sets, *Archiv Math.* **47** (1986), 279–280.
10. D. JUNGNICKEL AND K. VEDDER, On the geometry of planar difference sets, *European J. Combin.* **5** (1984), 143–148.
11. H. P. KO, A note on extraneous multipliers for difference sets, submited for publication.
12. H. P. KO AND D. K. RAY-CHAUDHURI, Multiplier theorems, *J. Combin. Theory Ser. A* **30** (1981), 134–157.
13. H. P. KO AND D. K. RAY-CHAUDHURI, Intersection theorems for group divisible difference sets, *Discrete Math.* **39** (1982), 37–58.
14. E. S. LANDER, "Symmetric Designs—An Algebraic Approach," Cambridge Univ. Press, Cambridge, 1983.
15. H. B. MANN, Balanced incomplete block designs and abelian difference sets, *Illinois J. Math.* **8** (1964), 252–261.
16. A. POTT, An affine analogue of Wilbrink's theorem, *J. Combin. Theory Ser. A*, in press.
17. A. POTT, On abelian difference sets with multiplier -1, *Archiv Math.*, in press.
18. H. WILBRINK, A note on planar difference sets, *J. Combin. Theory Ser. A* **38** (1985), 94–95.